

REMARKS

Claims 1-65 are pending, and all stand rejected. The independent claims are claims 1, 29, 30, 58, 59, 60, and 65. All of the independent claims are now amended without prejudice, in order to clarify that signing the certificate establishes the identity of the user in the second system. This is fully supported by the specification as originally filed, and introduces no new matter.

Claim 30 is not Indefinite

The final Office Action stated (at page 2) that claim 30 is indefinite under 35 USC §112, but the Advisory Action did not mention indefiniteness of claim 30. The final Office Action suggested the following alternative language: “ wherein the device of the second system has means for receipt of said information from the first device...” Applicant respectfully reiterates that claim 30 should remain as amended on September 1, 2005. In other words, it is correct and definite for claim 30 to say, “ wherein the device of the second system has means for receipt of said information from the second device.” After all, the “ second device” is part of the first system. Applicant points out that the “ device of the second system” is the first device. Thus, claim 30 properly says that the first device is “ a device forming part of the second system.”

Brief Summary of the Present Invention

The invention includes a method allowing user identification or data encryption with a public key technique, for a user who already has a certificate and corresponding secret key for signatures using another system. For example, a temporary key can be used by allowing the user to create acceptable certificates for those temporary keys. According to other (e.g. prior art) methods, such user-created certificates are not considered valid. In an embodiment of the present invention, user-created certificates are accepted, but they use the identity from a certificate already provided by a certificate authority (CA).

The Amended Independent Claims are Not Anticipated or Suggested by *Sudia*

It is respectfully believed that the present amendments clarify the very large difference between the present invention and the *Sudia* reference. As the Office Action states, the Signing Device 1 is located in the first system of present claim 1. Present claim 1 states that the second system generates a certificate for the key. However, column 13, line 66 of *Sudia* specifically says that the certificate is generated by Signing Device 1 (in the first system rather than the second system). Thus, this element of present claim 1 is not present in *Sudia*.

In col. 14, lines 14-34 of *Sudia*, the key share is used to partially sign the unsigned certificate that the Signing Device 1 sent to Signing Device 2. Thus, Signing Device 2 does not generate a certificate for the key share.

It is unsurprising that the cited portions of *Sudia* do not teach elements of the present independent claims. Generally speaking, *Sudia* is directed at a system having a plurality of signing devices, each of which possesses a “share” of a signature key. Thus, all of the shares are needed in order to form a final key for a final signature (see Abstract of *Sudia*). This is very different from the present claimed invention. As mentioned in the previous Office Action response, there is no teaching or suggestion in *Sudia* of a user of a second system authenticating its identify by having an authenticated identity in a first system. What *Sudia* is directed to is a technique in which a partial system wide authority (SWA) signature uses the SWA signature key share of multiple signing devices in order to generate a signed certificate.

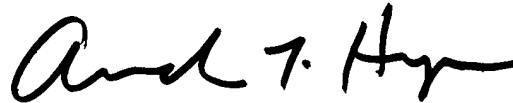
Applicant respectfully notes that authorization and authentication are two different things. The present claim 1 is directed to authenticating the user of a second system where the user has an authenticated identity in a first system.

Applicant also incorporates by reference the various arguments already submitted in Applicant’ s response of September 1, 2005. The arguments presented herein regarding claim 1 also apply to the other independent claims.

944-005.002
10/090,422

It is therefore respectfully submitted that claims 1-65, as presently amended, are believed to be distinguished over the cited art and that the claims are therefore in condition for allowance. Such action is earnestly solicited.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Andrew T. Hyman". The signature is fluid and cursive, with the first name "Andrew" being more prominent and the last name "Hyman" following in a similar style.

Andrew T. Hyman
Attorney for the Applicant
Registration No. 45,858

April 21, 2006
ATH/mbh
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, PO Box 224
Monroe CT 06468
(203) 261-1234